

L Number	Hits	Search Text	DB	Time stamp
1	19513	gateway and (packet or datagram or file or data)	USPAT; EPO; JPO; DERWENT	2004/06/24 07:34
2	2017	IKE or internet adj2 key adj2 exchang\$5	USPAT; EPO; JPO; DERWENT	2004/06/24 07:34
3	385	IPSEC	USPAT; EPO; JPO; DERWENT	2004/06/24 07:35
4	45490	encrypt\$4 or cipher\$4 or encipher\$4	USPAT; EPO; JPO; DERWENT	2004/06/24 07:35
5	1279	firewall and (encrypt\$4 or cipher\$4 or encipher\$4)	USPAT; EPO; JPO; DERWENT	2004/06/24 07:35
6	3111	713/150.ccls. or 713/153.ccls. or 713/154.ccls. or 713/160.ccls. or 713/168.ccls. or 713/171.ccls. or 713/189.ccls. or 713/200.ccls. or 713/201.ccls.	USPAT; EPO; JPO; DERWENT	2004/06/24 07:37
7	0	713/709.ccls.	USPAT; EPO; JPO; DERWENT	2004/06/24 07:37
8	615	709/200.ccls.	USPAT; EPO; JPO; DERWENT	2004/06/24 07:38
9	3706	(713/150.ccls. or 713/153.ccls. or 713/154.ccls. or 713/160.ccls. or 713/168.ccls. or 713/171.ccls. or 713/189.ccls. or 713/200.ccls. or 713/201.ccls.) or 709/200.ccls.	USPAT; EPO; JPO; DERWENT	2004/06/24 07:38
10	570	diffie adj2 hellman	USPAT; EPO; JPO; DERWENT	2004/06/24 07:38
11	4124	((diffie adj2 hellman) or ((713/150.ccls. or 713/153.ccls. or 713/154.ccls. or 713/160.ccls. or 713/168.ccls. or 713/171.ccls. or 713/189.ccls. or 713/200.ccls. or 713/201.ccls.) or 709/200.ccls.))	USPAT; EPO; JPO; DERWENT	2004/06/24 07:39
12	748	(gateway and (packet or datagram or file or data)) and ((diffie adj2 hellman) or ((713/150.ccls. or 713/153.ccls. or 713/154.ccls. or 713/160.ccls. or 713/168.ccls. or 713/171.ccls. or 713/189.ccls. or 713/200.ccls. or 713/201.ccls.) or 709/200.ccls.))	USPAT; EPO; JPO; DERWENT	2004/06/24 07:39
13	84	IPSEC and ((diffie adj2 hellman) or ((713/150.ccls. or 713/153.ccls. or 713/154.ccls. or 713/160.ccls. or 713/168.ccls. or 713/171.ccls. or 713/189.ccls. or 713/200.ccls. or 713/201.ccls.) or 709/200.ccls.))	USPAT; EPO; JPO; DERWENT	2004/06/24 07:40
14	23	(IPSEC and ((diffie adj2 hellman) or ((713/150.ccls. or 713/153.ccls. or 713/154.ccls. or 713/160.ccls. or 713/168.ccls. or 713/171.ccls. or 713/189.ccls. or 713/200.ccls. or 713/201.ccls.) or 709/200.ccls.))) and (diffie adj2 hellman)	USPAT; EPO; JPO; DERWENT	2004/06/24 07:40

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

Web

Results 1 - 10 of about 25,100 for IPSEC and diffie hellman. (0.71 seconds)

The NetIP Security Resource - Diffie-Helman Article

... didn't realize it. If that VPN is operating on the IPsec standard, then Diffie-Hellman is certainly in use. To follow the standards ...
www.netip.com/articles/keith/diffie-heiman.htm - 27k - Cached - Similar pages

[PDF] A Review of the Diffie-Hellman Algorithm and its Use in Secure ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Diffie-Hellman in IPsec Internet Protocol Security (IPsec) is a protocol being developed by the IETF to incorporate secure communications into the IP network ...
www.sans.org/rr/papers/20751.pdf - Similar pages

[Ipsec] IKEv2 Diffie Hellman groups

... Index] [**Ipsec**] IKEv2 Diffie Hellman groups. To: "**IPsec WG (E-mail)**" ipsec@ietf.org; Subject: [**Ipsec**] IKEv2 Diffie Hellman groups; ...
www.sandelman.ottawa.on.ca/ipsec/2003/11/msg00638.html - 5k - [Cached](#) - [Similar pages](#)

Diffie-Hellman Group 5 -Cisco IOS Software Releases 12.1 T - Cisco ...

... In this configuration, IPsec uses the 1536-bit Diffie-Hellman prime modulus group (group 5). Step 3. Router(config-crypto-map)#exit, ...
www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080161.html - 48k -
Cached - Similar pages

IPSec Overview Part One: General IPSec Standards

... **IPSec Overview Part One: General IPSec Standards**. By Andrew Mason. Article is provided courtesy of Cisco Press. Date: Feb 22, 2002. **Diffie-Hellman (DH)**. ... www.ciscopress.com/articles/article.asp?p=25470&pageNum=5 - 14k - Cached - Similar pages

Security Protocols Standards Diffie-Hellman

... Diffie-Hellman. In fact, if that VPN is operating on the IPSec standard, then Diffie-Hellman is certainly in use. The standards ...
security.ittoolbox.com/ nav/t.asp?t=390&p=390&h1=390 - 24k - Cached - Similar pages

What's New in Windows Server 2003 IPSec (Part 2)

... Specifically, we'll discuss each of the following: Computer startup security;
Stronger **Diffie-Hellman** group support; NAT traversal; Netsh **IPSec** context. ...
www.windowsecurity.com/articles/Windows_Server_2003_IPSec_Part2.html - 40k - Cached - Similar pages

TechTarget Discussions - Network Design

... Can you explain Diffie Hellman groups and how they work with triple
DES and IPsec?" Diffie-Hellman * post #278 * philmcg on 10/23/2001. ...
searchsecurity.discussions.techtarget.com/ WebX?msgInContext@54.azmpaUE4XQw.0@.ee83d5e/297 - 14k -
Cached - Similar pages

[Security Forums Dot Com :: View topic - Diffie-Hellman](#)

... Author, Message. **Ispsec** Espah Part-Time Guru Joined: 16 Mar 2003 Posts: 66, PostPosted: Mon Jan 26, 2004 8:17 pm Post subject: **Diffie-Hellman**, Reply with quote. ...
www.security-forums.com/forum/viewtopic.php?p=75759 - 43k - Cached - Similar pages

[PPT] Example: the Diffie-Hellman Key Exchange

File Format: Microsoft PowerPoint 97 - View as HTML
... the cryptographic core of the main authenticated **Diffie-Hellman** exchange of IKE (v1 and v2). 3. 03Crypto - Hugo Krawczyk. **IPSec**: IP Security [RFC2401-12]. ...
www.ee.technion.ac.il/~hugo/sigma.ppt - Similar pages




Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google

[Web](#)
[Images](#)
[Groups](#)
[News](#)
[Froogle](#)
[more »](#)



[Advanced Search](#)
[Preferences](#)

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

WebResults 1 - 10 of about 14,400 for IKE and diffie hellman. (0.41 seconds)**Configure an IKE Diffie-Hellman Group**

Configure an IKE Diffie-Hellman Group. Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a ...

www.juniper.net/techpubs/software/junos/junos57/swconfig57-getting-started/html/security-config48.html - 4k -

[Cached](#) - [Similar pages](#)

Diffie-Hellman Group 5 -Cisco IOS Software Releases 12.1 T - Cisco ...

... Configures an IKE policy with the 1536-bit Diffie-Hellman group (group 5). ... Use this command to specify the Diffie-Hellman group to be used in an IKE policy. ...

www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080161.html - 48k -

[Cached](#) - [Similar pages](#)

Configuring IKE

... these keys. See "Configuring IKE Pre-Shared (Authentication) Keys Manually".

e. Specify the Diffie-Hellman group identifier: isakmp ...

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/ipsec/conike.htm - 15k - [Cached](#) - [Similar pages](#)

[[More results from www.cisco.com](#)]

IKE Negotiation for IPSec Security : The Cable Guy, June 2002

... size). The Windows 2000 IKE module currently supports only Diffie-Hellman Oakley Group 1 (768 bits) and Group 2 (1024 bits). Although ...

www.microsoft.com/technet/community/columns/cableguy/cg0602.msp?frame=true - 48k - [Cached](#) - [Similar pages](#)

More Modular Exponential (MODP) Diffie-Hellman groups for Internet ...

... 10 Kivinen & Kojo Standards Track [Page 1] RFC 3526 MODP Diffie-Hellman groups for IKE May 2003 1. Introduction One of the important protocol parameters ...

www.ipa.go.jp/security/rfc/RFC3526EN.html - 20k - [Cached](#) - [Similar pages](#)

Security Protocols Standards Diffie-Hellman

... Within that framework is the Internet Key Exchange (IKE) protocol. IKE relies on yet another protocol known as OAKLEY, which uses Diffie-Hellman. ...

security.ittoolbox.com/nav/t.asp?t=390&p=390&h1=390 - 24k - [Cached](#) - [Similar pages](#)

Security Diffie-Hellman Public Key Distribution Scheme: Complete

... IKE relies on yet another protocol known as OAKLEY, which uses Diffie-Hellman. ... IKE relies on yet another protocol known as OAKLEY, which uses Diffie-Hellman. ...

security.ittooibox.com/documents/document.asp?i=939 - 20k - [Cached](#) - [Similar pages](#)

[PDF] A Review of the Diffie-Hellman Algorithm and its Use in Secure ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... the RFC, good, mid-level descriptions of the IPsec and IKE protocols can ... Diffie-Hellman in PKI Public Key Infrastructure (PKI) refers to a system of protocols ...

www.sans.org/rr/papers/20/751.pdf - [Similar pages](#)

[PPT] Example:the Diffie-Hellman Key Exchange

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... Rationale and development of SIGMA, the cryptographic core of the main authenticated Diffie-Hellman exchange of IKE (v1 and v2). 3. 03Crypto - Hugo Krawczyk. ...

www.ee.technion.ac.il/~hugo/sigma.ppt - [Similar pages](#)

Protocol Action: More MODP Diffie-Hellman groups for IKE to ...

... Protocol Action: More MODP Diffie-Hellman groups for IKE to Proposed Standard. From: The IESG; Subject: Protocol Action: More MODP ...

www.mail-archive.com/ipsec@lists.tislabs.com/msg00008.html - 6k - [Cached](#) - [Similar pages](#)



Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)


IKE and diffie hellman

Search

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

WebResults 1 - 10 of about 2,690 for IKE and diffie hellman and datagram. (0.43 seconds)**EllisTalks - Products - Video Series**

... **datagram** authenticated in Tunnel mode; Portions of IP **datagram** encrypted in Tunnel mode; An overview to **IKE** (Internet Key Exchange); The **Diffie-Hellman** method; The ...
 ellistalks.com/products/vol_III.html - 18k - [Cached](#) - [Similar pages](#)

[PDF] Ellis Talks - Video brochure TOC for Vol III - v2.inddFile Format: PDF/Adobe Acrobat - [View as HTML](#)

... in Tunnel mode; Portions of IP **datagram** encrypted in Tunnel mode. Internet Key Exchange — An overview to **IKE**; The **Diffie-Hellman** method algorithm explained ...
 ellistalks.com/pdf/JumpStart_Volume_III.PDF - [Similar pages](#)

Supported VPN Standards

... AH is embedded in the data to be protected (a full IP **datagram**). ... **Diffie-Hellman** is used within **IKE** to establish session keys. ...

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/ipsecstd.htm - 50k - [Cached](#) - [Similar pages](#)

Cisco - Packet[R] Magazine - April 2002 - Technology - Decoding ...

... STS) protocol allows two devices in the **Diffie-Hellman** exchange to ... of IPsec tunnels within the **IKE** protocol. ... header is attached, and the entire **datagram** can be ...

www.cisco.com/warp/public/784/packet/apr02/p29-technology.html - 25k - [Cached](#) - [Similar pages](#)

[[More results from www.cisco.com](#)]

818043 - L2TP/IPSec NAT-T update for Windows XP and Windows 2000

... It dynamically turns Internet Key Exchange (**IKE**) logging on ... L2TP - User **Datagram** Protocol (UDP) 500, UDP 1701; NAT-T ... 2048-Bit **Diffie-Hellman** Algorithm Update. ...
 support.microsoft.com/default.aspx?scid=kb;en-us;818043 - 26k - [Cached](#) - [Similar pages](#)

IPsec, isakmp, ike

... AH hashes on everything in the **datagram** including the ... The shared key is calculated using the **Diffie-Hellman** numbers ... The **IKE** SA is now established; Peer P sends a ...

www.rhysshaden.com/ipsec.htm - 46k - [Cached](#) - [Similar pages](#)

[PDF] Part III-bFile Format: PDF/Adobe Acrobat - [View as HTML](#)

... Security Protocol (WTLS, DSP) **Datagram** Security Protocol ... VPN) with security gateways n **IKE** is the ... defined based on **Diffie-Hellman** Encapsulation Decapsulation ...

www.itec.uni-klu.ac.at/~harald/multimedia/Vorlesung%20Part%20IIIb%20-%20Sec%20Apps.pdf - [Similar pages](#)

Dax Networks - Technology - Virtual Private Network

... Public key cryptography for signing the **Diffie-Hellman** exchanges to ... **IKE** should be used in most real-world ... Control Protocol [TCP] or User **Datagram** Protocol [UDP] ...

www.daxnetworks.com/Dax/Technology/VPN.htm - 31k - [Cached](#) - [Similar pages](#)

[PDF] Microsoft PowerPoint - VPN Technologies.pptFile Format: PDF/Adobe Acrobat - [View as HTML](#)

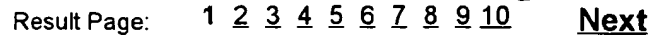
... IP Header TCP Header Data Original IP **Datagram** IP Header ... history – Initial two candidates for **IKE** • Photuris – using **Diffie-Hellman** key exchange ...

www.cs.ru.ac.za/courses/Honours/Networks/lectures/VPN%20Technologies-6up.pdf - [Similar pages](#)

[PPT] Networkers TemplateFile Format: Microsoft Powerpoint 97 - [View as HTML](#)

... Confidentiality through encryption of IP **datagram**. Integrity ... key. **IKE** provides PFS if required by using **Diffie-Hellman** for each re-key. If ...

www.csc.calpoly.edu/~husmith/CPE465-spring-02/Cisco_slides.ppt - [Similar pages](#)



Search

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

h g g e c e ch h e e

ff e he